AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
5537 Canfield Pl N, Seattle, Washington

Case No. MJ13-608

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
5537 Canfield Pl N, Seattle, Washington, as further described in Attachmetn A to the Attached affidavit

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachmetn B to Attached Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 2252	Possession of Child Pornography
18 USC 2260	Production of Sexually Explicit Depictions of Minors for importation into the US

The application is based on these facts:
See attached affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Scott Sutehall, SA HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: 12/12/13

Judge's signature

City and state: Seattle, WA

Magistrate Judge Brian A Tsuchida
Printed name and title

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I. INTRODUCTION

I, Scott Sutehall, being first duly sworn on oath, depose and say:

1. I am a Special Agent (SA) with the U.S. Department of Homeland Security, Homeland Security Investigations (HSI), assigned to the Seattle, Washington field office. I have been an agent with HSI since March 2008. HSI is responsible for enforcing the customs and immigration laws and federal criminal statutes of the United States. I joined the Child Exploitation Unit in May 2013, although I previously assisted in other child exploitation cases before joining the unit. As part of my duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography and material involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252(a), and 2252A(a). I am a graduate of the Federal Law Enforcement Training Center (FLETC), HSI Special Agent Training Program, and have received further specialized training in investigating child pornography and child exploitation crimes. I have also had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256(8)). I have participated in the execution of previous search warrants which involved child exploitation and/or child pornography offenses and the search and seizure of computers and other digital devices. I am a member of the Seattle Internet Crimes Against Children (ICAC) Task Force in the Western District of Washington, and work with other federal, state, and local law

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

enforcement personnel in the investigation and prosecution of crimes involving the sexual exploitation of children.

2. I make this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the residence located at 5537 Canfield Place N., Seattle, Washington, (hereinafter the "SUBJECT PREMISES"), more fully described in Attachment A to this Affidavit, for the things specified in Attachment B to this Affidavit, for the reasons set forth below.

3. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation, including those provided to me by the Royal Canadian Mounted Police; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

4. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are relevant to the determination of probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2251(a) (Production of Child Pornography); 18 U.S.C. § 2252 (Possession of Child Pornography and 18 U.S.C. § 2260 (Production of Sexually Explicit Depictions of a Minor For Importation into the United States) will be found at the SUBJECT PREMISES.

II. INVESTIGATION

5. On December 11, 2013, I learned from SA Russell Simmons, the HSI Representative at the United States Consulate General in Vancouver, Canada, that

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

JASON CHRISTOPHER PAUR had been arrested at the Silver Star Resort near Vernon, British Columbia, pursuant to a charge of Voyeurism per Section 162(1) of the Canadian Criminal Code, as well as Making and Possessing Child Pornography. JASON CHRISTOPHER PAUR is a United States citizen with permanent residence in Seattle, Washington, at 5537 Canfield Place N, Seattle, Washington (the SUBJECT PREMISES).

6. JASON CHRISTOPHER PAUR is employed pursuant to a coaching contract by The Bush School, an independent K-12 school located in Madison Valley, Seattle. JASON CHRISTOPHER PAUR works as the Head Varsity Coach for the school's Cross-Country Skiing Varsity Co-Ed team, and the Cross Country Running Girls and Boys Varsity teams. JASON CHRISTOPHER PAUR has been employed by The Bush School as a coach for over 15 years.

7. As part of the Cross County Skiing Coed team's winter schedule, the team departed to the Silver Star resort in British Columbia on December 8, 2013 for a five day Winter Training session at the resort. The team members stayed in accommodations at the resort.

8. I learned the following information from an RCMP official report and from my conversations with RCMP officers.

9. On December 10, 2013 at 10.25 p.m., a Chaperon, J.B. called RCMP Officer Richard Lausman from 23-9885 Pinnacles Rd. in Vernon, British Columbia to report that he was in Vernon, BC with a school group of skiers from Seattle, Washington on a ski trip staying at Silver Star Mountain. The group consisted of nine females (aged 14 to 20), two males (aged 17 and 18), the Head Coach, JASON CHRISTOPHER PAUR, and Chaperones R.C. and J.B. The group arrived at the ski resort on December 8, 2013, and were planning on staying in the area until Friday, December 13, 2013.

10. The group was staying together in a Chalet at the Pinnacles consisting of shared kitchen and living room area, and shared, but separated bedrooms. Six of the females shared a room on the 3rd floor and three of the females shared a room on the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

second floor. The two young males shared a room on the second floor and the Chaperones all shared a room on the 3rd floor.

11. J.B. reported that the three females on the second floor, Victim 1, Victim 2 and Victim 3 discovered a camera that was recording video sitting on the window sill partially hidden by the curtains. Victims 1, 2 and 3 are all minors between the ages of 14 and 16. Victim 1 was the first to see the camera and picked it up thinking it was a prank. Victims 1, 2 and 3 stopped the camera from recording and briefly viewed part of one of the videos. Victims 1, 2 and 3 saw on the video that the camera was being set-up by their Head Coach, JASON CHRISTOPHER PAUR in the other females' bedroom on the 3rd floor. They did not view the video any further, but brought the camera to Female 1 who was one of the females from the 3rd floor bedroom. Female 1 also briefly viewed the video and brought it to the attention of the Chaperones, J.B. and R.C.

12. R.C. confronted JASON CHRISTOPHER PAUR and seized the camera. R.C. later stated to RCMP Officer Lausman that JASON CHRISTOPHER PAUR told R.C. that JASON CHRISTOPHER PAUR set the camera up in the females' bedrooms. J.B. then called the police. The Chaperones decided to separate JASON CHRISTOPHER PAUR from the youth. R.C. drove JASON CHRISTOPHER PAUR with his belongings to the Sheraton Hotel near the Kelowna Airport. R.C. took charge of the camera and called the police, waiting for attendance.

13. At 11.23 p.m. Officer Lausman arrived at the 23-9885 Pinnacles Rd on Silver Star Mountain and met J.B. J.B. handed Officer Lausman the camera. J.B. said that neither he nor R.C. viewed any of the video. Officer Lausman took the camera, which was a Panasonic LUMIX digital camera (hereinafter the "Digital Camera"), which had a video stopped on the view screen.

14. Officer Lausman played the video on the Digital Camera. Officer Lausman viewed a short sequence of the video showing a male setting the camera up to shoot video of the 3rd Floor female bedroom. The male shows his face in the video and Officer

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Lausman had J.B. review the video and confirm this male was indeed JASON CHRISTOPHER PAUR.

15. Officer Lausman continued to view the video and observed that once JASON CHRISTOPHER PAUR leaves the bedroom, a young female is seen coming out of the bathroom only wearing a towel. The female proceeded to get dressed and unknowingly exposes her naked body to this camera. Officer Lausman immediately stopped viewing this video.

16. At 11.23 p.m. Officer Lausman seized the camera as evidence and locked it in his patrol car to continue the investigation. Officer Lausman then met with Victims 1, 2 and 3, and went with them to the 2nd floor bedroom where the Digital Camera was found. The Digital Camera was found on the window sill by the curtain.

17. Officer Lausman then briefly met with Female 1, and then accompanied her up to the 3rd floor bedroom. This bedroom appeared the same as the one on the video on the Digital Camera that Officer Lausman initially viewed. From the perspective of the video, the camera had been situated by the window sill. Victim 4, a minor under the age of 18 years, was staying in the 3rd floor bedroom.

18. Two RCMP officers arrested JASON CHRISTOPHER PAUR at the Sheraton Hotel where he had been taken earlier by R.C. Officer Lausman took custody of JASON CHRISTOPHER PAUR at 1.57 a.m. and transported him to Vernon Cells to be booked.

19. Officer Lausman retrieved that Digital Camera from his patrol car. Officer Lausman viewed the contents of the Camera which were contained on an 8gb Kodak Secure Digital (SD) card.

The Panasonic Lumix Digital Camera

20. The Digital Camera is a Panasonic Lumix Digital Camera, capable of downloading images and video files to other digital devices including computers. The

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

following is an excerpt from a Panasonic Press release regarding the original 2002 Panasonic Lumix Digital Camera[1]:

> Not only do these cameras produce high-quality, professional-looking digital photographs, but their convenient, user-friendly features make multimedia applications quick and easy. Featuring built-in USB ports1 and SD Memory Card slots, the . . . digital cameras also offer consumers networking versatility with PCs and a wide variety of compatible SD-enabled devices.
>
> . . .
>
> Digital images can be downloaded to a PC or removable memory card, transferred to CD-Rs, printed out, viewed on a TV or computer screen, or attached to an e-mail message. With digital cameras, taking the picture is just the start of the creative process. Advanced digital technology and networking capability let consumers enjoy their beautiful photos in exciting new ways.
>
> The magic of digital technology makes it easy for anyone to edit and enhance their images with the included ArcSoftä photo editing software. Using a photo editing web site like PictureStage.com, consumers can also store their photos in personal, online albums; create printed materials such as posters or calendars featuring their images; or have their photos printed on gifts like t-shirts and coffee mugs.
>
> The Lumix cameras feature a memory card slot that is compatible with either SD Memory Cards or a MultiMediaCard.™ An 8MB, 16MB or 32MB SD Memory Card, depending upon the model, is included with each Lumix camera. About the size of a postage stamp, the SD card features large storage, great flexibility, excellent security and fast data transfer. The medium allows for the quick, easy exchange of images, music, video and slide presentations among a growing number of SD Memory Card-enabled

---

[1] The press release was obtained from website: http://www.dpreview.com/news/2002/01/11/panasoniclumix?utm_campaign=internal-link&utm_source=news-list&utm_medium=text&ref=title_19, on December 12, 2013.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

devices, including audio products, camcorders, memo recorders and handheld computers and PDAs.

SUBJECT's Use of Digital Devices

21. On December 11, 2013, I learned from officials at the Bush School that JASON CHRISTOPHER PAUR uses a school issued email account to enable communications with parents, school officials and students. This email address is publically available on the Bush School website. Bush School official also provided me with a personal email address for JASON CHRISTOPHER PAUR. Bush School officials confirmed that JASON CHRISTOPHER PAUR has not been provided with a Bush School computer or laptop.

22. RCMP identified a laptop and cellphone as belonging to JASON CHRISTOPHER PAUR and secured those items.

The SUBJECT RESIDENCE

23. On December 11, 2013, a WSDOL official provided me with the driver license issued to JASON CHRISTOPHER PAUR. The license listed an address of 5537 Canfield Place N, Seattle, Washington (the SUBJECT PREMISES).

24. On December 11, 2013, I conducted a query of publicly available databases, which revealed that JASON CHRISTOPHER PAUR currently resides at the SUBJECT PREMISES. On December 11, 2013, I reviewed JASON CHRISTPOPHER PAUR's personnel file at The Bush School. The file contained a medical examiners' certificate for JASON CHRISTOPHER PAUR dated September 6, 2013. The card listed the address of the SUBJECT RESIDENCE as JASON CHRISOTPHER PAUR's home address.

25. On December 11, 2013, JASON CHRISTOPHER PAUR provided the RCMP with the address of his residence in Seattle, Washington, which was the Subject Residence.

III. DEFINITIONS AND TECHNICAL TERMS

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

26. Set forth below are some definitions of technical terms, most of which are used throughout this Affidavit pertaining to the Internet and computers generally.

a. Computers and digital devices: As used in this Affidavit, the terms "computer" and "digital device," along with the terms "electronic storage media," "digital storage media," and "data storage device," refer to those items capable of storing, creating, transmitting, displaying, or encoding electronic or digital data, including computers, hard drives, thumb drives, flash drives, memory cards, media cards, smart cards, PC cards, digital cameras and digital camera memory cards, electronic notebooks and tablets, smart phones and personal digital assistants, printers, scanners, and other similar items.

b. Internet Service Providers (ISPs) and the storage of ISP records: Internet Service Providers are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs maintain records ("ISP records") pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use.

IV. PRIOR EFFORTS TO OBTAIN EVIDENCE

27. Any other means of obtaining the necessary evidence to prove the elements of computer/Internet-related crimes, for example, a consent search, could result in an unacceptable risk of the loss/destruction of the evidence sought. If agents pursued a consent-based interview of and/or a consent-based search of JASON CHRISTOPHER

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

PAUR's digital media, JASON CHRISTOPHER PAUR could rightfully refuse to give consent and arrange for destruction of all evidence of the crime before agents could return with a search warrant. Based on my knowledge, training and experience, the only effective means of collecting and preserving the required evidence in this case is through a search warrant. Based on my knowledge, no prior search warrant has been obtained to search the SUBJECT PREMISES.

V. TECHNICAL BACKGROUND

28. As part of my training, I have learned that producers of child pornography can produce both still and moving images directly from the average video or digital camera. These still and/or moving images are then uploaded from the camera to a computer, either by attaching the camera to the computer through a USB cable or similar device, or by ejecting the camera memory card from the camera and inserting it into a card reader. Once uploaded to the computer, the images can then be stored, manipulated, transferred, or printed directly from a computer.

29. Digital images can then be edited in ways similar to those by which a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production is a difficult trail for law enforcement to follow.

30. As part of my training, I have become familiar with the Internet, a global network of computers and other electronic devices that communicate with each other using various means, including standard telephone lines, high speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions, including satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via email.

31. I know, based on my training and experience, that cellular phones (referred to herein generally as "smart phones") have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smart phone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smart phone can also easily plug the device into a computer or a video camera, via a USB cable, and transfer data files from one digital device to another.

32. As set forth above and in Attachment B to this Affidavit, I seek permission to search for and seize evidence, fruits, and instrumentalities of the above-referenced crimes that might be found at the SUBJECT PREMISES in whatever form they are found. It has been my experience that individuals involved in child pornography often prefer to store images of child pornography in electronic form. The ability to store images of child pornography in electronic form makes digital devices, examples of which are enumerated in Attachment B to this Affidavit, an ideal repository for child pornography because the images can be easily sent or received over the Internet. As a result, one form in which these items may be found is as electronic evidence stored on a digital device.

a. Based upon my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that computers and computer technology have revolutionized the way in which child pornography is collected, distributed, and produced. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these images was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation would follow the same paths. More recently, through the use of computers and the Internet, distributors of child pornography use membership based/subscription based websites to conduct business, allowing them to remain relatively anonymous.

b. In addition, based upon my own knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that the development of computers has also revolutionized the way in which those who seek out child pornography are able to obtain this material. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage. More specifically, the development of computers has changed the methods used by those who seek to obtain access to child pornography as described in subparagraphs (c) through (e) below.

c. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers, including ISPs, allow email service between subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet. Having said that, however, this application does not seek to reach any host computers.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

This application seeks permission only to search the computers and related computer media found at the SUBJECT PREMISES.

d. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography, and (ii) websites that offer images of child pornography. Those who seek to obtain images or videos of child pornography can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions involving those who wish to gain access to child pornography over the Internet. Sometimes the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the distributor's/recipient's computer, including the Internet history and cache to look for "footprints" of the websites and images accessed by the distributor/recipient.

e. The computer's capability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as a "hard drive") used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 1 terabyte are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage elsewhere. Once this is done, there is no readily apparent evidence at the "scene of the crime." Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

33. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in child pornography:

a. Those who produce, receive and attempt to receive child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Those who produce, receive and attempt to receive child pornography may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts. These individuals may keep records, to include names, contact information, and/or dates of these interactions, of the children they have attempted to seduce, arouse, or with whom they have engaged in the desired sexual acts.

c. Those who produce, receive and attempt to receive child pornography often possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain these "hard copies" of child pornographic material for many years.

d. Likewise, those who produce, receive and attempt to receive child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

collections are often maintained for several years and are kept close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly.

e. Those who produce, receive and attempt to receive child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Those who receive and attempt to receive child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. In this case, based on the conduct of JASON CHRISTOPHER PAUR in secreting a video camera positioned to capture videos of naked minor females, who were students in his care, I believe that JASON CHRISTOPHER PAUR may be a producer and collector of child pornography who stores and collects videos and images of minors engaged in sexually explicit conduct on digital devices. Based on my knowledge, training and experience, and in my dealings with other law enforcement officers who investigate child exploitation violations, I also believe that JASON CHRISTOPHER PAUR saves his collection of child pornography on a variety of digital media devices, including mobile and/or portable digital devices.

34. Based on my training and experience, and that of computer forensic agents that I work and collaborate with on a daily basis, I know that every type and kind of information, data, record, sound or image can exist and be present as electronically stored information on any of a variety of computers, computer systems, digital devices, and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

other electronic storage media. I also know that electronic evidence can be moved easily from one digital device to another. As a result, I believe that electronic evidence may be stored on any digital device present at the SUBJECT PREMISES.

35. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I know that in some cases the items set forth in Attachment B may take the form of files, documents, and other data that is user-generated and found on a digital device. In other cases, these items may take the form of other types of data - including in some cases data generated automatically by the devices themselves.

36. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I believe that if digital devices are found in the SUBJECT PREMISES there is probable cause to believe that the items set forth in Attachment B will be stored in those digital devices for a number of reasons, including but not limited to the following:

a. Once created, electronically stored information (ESI) can be stored for years in very little space and at little or no cost. A great deal of ESI is created, and stored, moreover, even without a conscious act on the part of the device operator. For example, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache," without the knowledge of the device user. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes affirmative steps to delete them. This ESI may include relevant and significant evidence regarding criminal activities, but also, and just as importantly, may include evidence of the identity of the device user, and when and how the device was used. Most often, some affirmative action is necessary to delete ESI. And even when such action has been deliberately taken, ESI can often be recovered, months or even years later, using forensic tools.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. Wholly apart from data created directly (or indirectly) by user-generated files, digital devices - in particular, a computer's internal hard drive - contain electronic evidence of how a digital device has been used, what is has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible for a user to use such specialized software to delete this type of information - and, the use of such special software may itself result in ESI that is relevant to the criminal investigation. HSI agents in this case have consulted on computer forensic matters with law enforcement officers with specialized knowledge and training in computers, networks, and Internet communications. In particular, to properly retrieve and analyze electronically stored (computer) data, and to ensure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the computers. To effect such accuracy and completeness, it may also be necessary to analyze not only data storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the computer and software.

VII. SEARCH AND/OR SEIZURE OF DIGITAL DEVICES

37. In addition, based on my training and experience and that of computer forensic agents that I work and collaborate with on a daily basis, I know that in most cases it is impossible to successfully conduct a complete, accurate, and reliable search for electronic evidence stored on a digital device during the physical search of a search site for a number of reasons, including but not limited to the following:

a. Technical Requirements: Searching digital devices for criminal evidence is a highly technical process requiring specific expertise and a properly

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

controlled environment. The vast array of digital hardware and software available requires even digital experts to specialize in particular systems and applications, so it is difficult to know before a search which expert is qualified to analyze the particular system(s) and electronic evidence found at a search site. As a result, it is not always possible to bring to the search site all of the necessary personnel, technical manuals, and specialized equipment to conduct a thorough search of every possible digital device/system present. In addition, electronic evidence search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since ESI is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code embedded in the system such as a "booby trap"), a controlled environment is often essential to ensure its complete and accurate analysis.

b. Volume of Evidence: The volume of data stored on many digital devices is typically so large that it is impossible to search for criminal evidence in a reasonable period of time during the execution of the physical search of a search site. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Computer hard drives are now being sold for personal computers capable of storing up to two terabytes (2,000 gigabytes of data.) Additionally, this data may be stored in a variety of formats or may be encrypted (several new commercially available operating systems provide for automatic encryption of data upon shutdown of the computer).

c. Search Techniques: Searching the ESI for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement personnel with appropriate expertise may need to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or peruse every file briefly to determine whether it falls within the scope of the warrant.

38. In this particular case, the government anticipates the use of a hash value library to exclude normal operating system files that do not need to be searched, which will facilitate the search for evidence that does come within the items described in Attachment B. Further, the government anticipates the use of hash values and known file filters to assist the digital forensics examiners/agents in identifying known and or suspected child pornography image files. Use of these tools will allow for the quick identification of evidentiary files but also assist in the filtering of normal system files that would have no bearing on the case.

39. Because multiple people may share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain computers that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents conducting the search find multiple computers in the residence, they will attempt to corroborate, on site, which resident(s) has/have access to each computer. If agents are able to conclusively determine, on site, that JASON CHRISTOPHER PAUR does not use or have access to a particular computer or digital device, agents will not seize that particular computer or digital device pursuant to this warrant. However, if agents conducting the search nonetheless determine that it is probable that the things described in this warrant could be found on any computer(s) or digital device(s) in the residence, this application seeks permission to conduct an onsite search of those computers and digital devices as well, using forensic software, to determine if any child pornography is present. If, as a result of this onsite search, there is no child pornography present on those computers or digital devices, then they will not be searched further and will not be

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

seized. However, agents will be authorized to seize any computer or digital device owned or predominantly used by JASON CHRISTOPEHR PAUR for off-site forensic review, if an onsite forensic review is not possible or feasible.

40. In accordance with the information in this Affidavit, law enforcement personnel will execute the search of digital devices seized pursuant to this warrant as follows:

a. Upon securing the search site, the search team will conduct an initial review of any digital devices/systems to determine whether the ESI contained therein can be searched and/or duplicated on site in a reasonable amount of time and without jeopardizing the ability to accurately preserve the data.

b. If, based on their training and experience, and the resources available to them at the search site, the search team determines it is not practical to make an on-site search, or to make an on-site copy of the ESI within a reasonable amount of time and without jeopardizing the ability to accurately preserve the data, then the digital devices will be seized and transported to an appropriate law enforcement laboratory for review and to be forensically copied ("imaged"), as appropriate.

c. In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will produce a complete forensic image, if possible and appropriate, of any digital device that is found to contain data or items that fall within the scope of Attachment B of this Affidavit. In addition, appropriately trained personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data fall within the list of items to be seized pursuant to the warrant. In order to search fully for the items identified in the warrant, law enforcement personnel, which may include investigative agents, may then examine all of the data contained in the forensic image/s and/or on the digital devices to view their precise contents and determine whether the data fall within the list of items to be seized pursuant to the warrant.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

d. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this Affidavit.

e. If, after conducting its examination, law enforcement personnel determine that any digital device is an instrumentality of the criminal offenses referenced above, the government may retain that device during the pendency of the case as necessary to, among other things, preserve the instrumentality evidence for trial, ensure the chain of custody, and litigate the issue of forfeiture. If law enforcement personnel determine that a device was not an instrumentality of the criminal offenses referenced above, it shall be returned to the person/entity from whom it was seized within 90 days of the issuance of the warrant, unless the government seeks and obtains authorization from the court for its retention.

41. In order to search for ESI that falls within the list of items to be seized pursuant to Attachment B to this Affidavit, law enforcement personnel will seize and search the following items (heretofore and hereinafter referred to as "digital devices"), subject to the procedures set forth above:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any digital device used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, cameras, encryption devices, and optical scanners;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or memory buffers, smart cards, PC cards, memory sticks, flashdrives, thumb drives, camera memory cards, media cards, electronic notebooks, and personal digital assistants;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device, or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the device hardware, or ESI to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the digital device, or ESI; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the digital device or ESI.

VIII. CONCLUSION

42. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of instrumentalities of violations of 18 U.S.C. § 2251(a) (Production of Child Pornography); 18 U.S.C. § 2252 (Possession of Child Pornography) and 18 U.S.C. § 2260 (Production of Sexually Explicit Depictions of a Minor For Importation into the United States) are located at the SUBJECT PREMISES, as more fully described in Attachment A to this Affidavit, as well as on and in any digital

///

///

///

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

devices found therein. I therefore request that the court issue a warrant authorizing a search of the SUBJECT PREMISES for the items more fully described in Attachment B hereto, incorporated herein by reference, and the seizure of any such items found therein.

Dated this 12 day of December, 2013.

Scott Sutehall, Affiant
Special Agent
Department of Homeland Security
Homeland Security Investigations

SUBSCRIBED and SWORN to before me this 12 day of December, 2013.

BRIAN A. TSUCHIDA
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

Description of Property to be Searched

i) The physical address of the SUBJECT PREMISES is 5537 Canfield Place N., Seattle, Washington and can be more fully described as a single family residence one story green bungalow with white trim, with wooden painted siding, and a detached garage. There is an aluminum screen in front of the whit front door. The number "5537" is at the base of the front door.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

ITEMS TO BE SEIZED

The following records, documents. files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2251(a) (Production of Child Pornography); 18 U.S.C. § 2252 (Possession of Child Pornography) and 18 U.S.C. § 2260 (Production of Sexually Explicit Depictions of a Minor For Importation into the United States) which may be found at the SUBJECT PREMISES:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct, in any format or media.

2. Evidence of the installation and use of P2P software, and any associated logs, saved user names and passwords, shared files, and browsing history;

3. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

6. Any and all address books, names, lists of names, telephone numbers, and addresses of minors;

7. Any and all diaries, notebooks, notes, non-pornographic pictures of children, and any other records reflecting personal contact or other activities with minors;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

8. Any receipts, manuals or records regarding the Panasonic Lumix Digital Camera (Digital Camera).

9. Any non-digital recording devices and non digital media capable of storing images and videos.

10. Digital devices and/or their components, which include, but are not limited to:

a. Any digital devices and storage device capable of being used to commit, further, or store evidence of the offense listed above;

b. Any digital devices used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or memory buffers, smart cards, PC cards, memory sticks, flashdrives, thumb drives, camera memory cards, media cards, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

11. Evidence of who used, owned or controlled any seized digital device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history;

12. Evidence of malware that would allow others to control any seized digital device(s) such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malware; as well as evidence of the lack of such malware;

13. Evidence of the attachment to the digital device(s) of other storage devices or similar containers for electronic evidence;

14. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from a digital device;

15. Evidence of times the digital device(s) was used;

16. Any other ESI from the digital device(s) necessary to understand how the digital device was used, the purpose of its use, who used it, and when.

The seizure of digital devices and/or their components as set forth herein is specifically authorized by this search warrant, not only to the extent that such digital devices constitute instrumentalities of the criminal activity described above, but also for the purpose of the conducting off-site examinations of their contents for evidence, instrumentalities, or fruits of the aforementioned crimes.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970